REMARKS

Status of the Claims

- Claims 1, 5-10, and 12-17 are pending in the Application.
- Claims 1, 5-10, and 12-17 are rejected by the Examiner.

Claim Rejections Pursuant to 35 U.S.C. §102

Claims 1-2 and 4-17 stand rejected pursuant to 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 6,061,449 to Candelore et al. The Applicants respectfully traverse the rejection.

Candelore et al. discloses an apparatus for securely communicating encrypted, or authenticated, blocks of program information or re-ordered fields of program information between a storage device and a secure processing circuit in cipher block chains. (col. 10, line 66 through col. 11 line 9).

Claim 1 recites:

> A method of generating a machine identifier comprising:
> generating a database of records comprising object identifiers, each record having an associated memory block location;
> randomly deleting records in the database, the memory locations of the deleted records becoming available for allocation;
> allocating a file comprising memory blocks of the memory locations of the deleted records, each of the blocks having an object identifier based on the block's location in a memory; and
> creating a machine identifier based on the object identifiers of the deleted records associated with the allocated memory block locations.

Applicant submits that Candelore et al. does not disclose all elements of independent Claim 1. As stated on page 6 of the Applicant's response dated 1/12/06: "Candelore et al. does not disclose the generation of a database of records comprising object identifiers and randomly deleting records in the database. In addition, Candelore et al. does not disclose the generation of a machine identifier from the object identifier of the randomly deleted records."

Applicant respectfully re-submits this statement because Applicant is unable to locate the missing elements even in light of the specific citations provided by the Examiner. Specifically, in the "Response to Arguments" section on page 2 of the Office Action dated 4/3/6, the Examiner rejects Applicant's argument that Candelore et al. does not disclose the

generation of a database of records comprising object identifiers and randomly deleting records in the database by citing to col. 19, lines 36-43 and col. 24 lines 46-67 as well as col. 2 lines 9-16. However, none of these cited sections teaches the random deletion of records in a database as part of the generation of a machine identifier. No teaching is found concerning the random deletion of database records at all. Specifically, Candelore et al. at the above-cited locations teaches:

> "Program information refers generically to any information that is used by the secure circuit in the execution of a program. This may include instructions such as operational codes (op-codes) in machine code, or pseudo code or interpreted code, such as Java.TM.. It may include look-up tables, stored keys, and various temporary data such as intermediate calculations and the state of the secure circuit." (col 2, lines 9-16).
>
> "Furthermore, the address lines of the external storage device may be scrambled such that sequential blocks of the program information are stored non-sequentially. That is, the bytes, which may each include eight bits, for example, can be stored in non-sequential address locations of the storage. Thus, the external storage device 110 is said to be a scrambled memory. A key may be used here as well. A key may be different on a group or unit basis." (col. 19, lines 36-43).
>
> "Address-dependent decryption and authentication of the program information can prevent a pirate from moving otherwise properly encrypted and authenticated block chains around in storage device to get the decoder to process program information out of sequence. Such out-of-sequence processing could cause the descrambling receiver to improperly grant access to and descramble a data transmission.
> If possible, the key used for encryption and decryption and/or authentication should have both address dependent scrambling and unit key dependence. The unit key is a key that is unique to each decoder and may depend on, for example, the decoder serial number which is provided at the time of manufacture. Thus, it is desirable for the key to depend on individual units, or groups of individual units. Otherwise, it may be possible for a pirate to read the scrambled key data in the external storage device from one unit, and then place that same scrambled key into another unit's external storage device. This might be a way for a pirate to clone authorization to services between units and must be prevented.
> Address dependent scrambling and unit key dependence also prevents knowledge of a key used to authenticate and/or scramble a block of program information in one decoder to be used in another decoder." (col. 24 line 46 through col. 25 line 2).

Applicant notes that the specific teaching of randomly deleting records in a database is completely absent from the above-cited and reproduced paragraphs of Candelore et al.. Indeed, Applicant cannot find any teaching of random deletion of records in a database

anywhere in Candelore et al. Accordingly, Candelore does not teach the Claim 1 element of randomly deleting records in the database. Applicant also submits that Candelore et al. also does not teach this element in the context of generating a machine identifier as recited in Claim 1.

The Examiner states that the citations in columns 2, 19, and 24 above teach "underlying functionality achieved by the use of the database is disclosed in the Candelore patent i.e. storing the program in non contiguous memory". Applicant respectfully disagrees that storing a program in non-contiguous memory is relevant to the specific recitation in Claim 1.

Applicant submits "underlying functionality" is not the standard used for 35 U.S.C. §102 anticipation. MPEP §2131 instructs that to anticipate a claim for purposes of a 35 U.S.C. §102 rejection, the reference must teach every element of the claim. Applicant submits that Candelore et al. does not expressly or inherently teach the generation of a database of records comprising object identifiers and randomly deleting records in the database as part of a method to generating a machine identifier as recited in Claim 1.

Applicant respectfully submits that Candelore et al. also does not inherently teach generation of a database of records comprising object identifiers and randomly deleting records in the database as part of a method to generating a machine identifier because Applicant can find no teaching in Candelore et al. which relies on such an element as an essential part of the invention of Candelore et al. Without a reliance that such an element is an essential and necessary part of the disclosure of Candelore et al., the teaching is not inherent. Since Candelore et al. does not assume the presence of, rely on the principles of, make an essential part of, or hint that deletion of database records is a necessary precursor to the teachings of Candelore et al., and since no extrinsic evidence is produced to support the necessity of a deletion of database records in the generation of a machine identifier, then that teaching cannot be inherent.

Continuing to address the Examiner's response on page 2 of the present Office Action dated 4/3/6, Applicant can find no teaching in Candelore et al. that specifically teaches a generation of a machine identifier from the object identifier of the randomly deleted records. The Examiner cites column 15, lines 42-50, Col. 19, lines 40-43, and col. 24, lines 54-67 and cites the "key" as the unique identifier which is dependent on randomly selected memory

addresses. However, none of these cited sections teaches generation of a machine identifier from the object identifier of the randomly deleted records. Specifically, Candelore et al. at the above-cited locations teaches:

> "In another aspect of the present invention, a secure circuit uses program information for generating a cryptographic key. The key may be used to descramble a data transmission in hardware. Depending on the partitioning of the secure circuit, the descrambling may be done internally or externally.
> The key may be generated and handed to a software module to descramble the data transmission. The software module may be internal to the secure circuit or external to the secure circuit." (col. 15, line 42-50).
> "Thus, the external storage device 110 is said to be a scrambled memory. A key may be used here as well. A key may be different on a group or unit basis." (col. 19, lines 40-43).
> "If possible, the key used for encryption and decryption and/or authentication should have both address dependent scrambling and unit key dependence. The unit key is a key that is unique to each decoder and may depend on, for example, the decoder serial number which is provided at the time of manufacture. Thus, it is desirable for the key to depend on individual units, or groups of individual units. Otherwise, it may be possible for a pirate to read the scrambled key data in the external storage device from one unit, and then place that same scrambled key into another unit's external storage device. This might be a way for a pirate to clone authorization to services between units and must be prevented.
> Address dependent scrambling and unit key dependence also prevents knowledge of a key used to authenticate and/or scramble a block of program information in one decoder to be used in another decoder." (col. 24 line 54 through col. 25 line 2).

Upon close examination of the above citations in Candelore et al., Applicants can find no language that supports a teaching of generation of a machine identifier from the object identifier of the randomly deleted records as recited in Claim 1. Page 2 of the Office Action dated 4/3/6 states that the "key" is the unique identifier. Yet, Applicant can find no teaching that the key is generated as a machine identifier from the object identifier of randomly deleted records. Candelore et al. teaches:

> "If possible, the key used for encryption and decryption and/or authentication should have both address dependent scrambling and unit key dependence. The unit key is a key that is unique to each decoder and may depend on, for example, the decoder serial number which is provided at the time of manufacture." (col. 24, lines 53-58).

Thus, the "key" is constructed using a second key termed a "unit key" and the unit key is constructed using the serial number at the time of manufacture. Claim 1 recites no such second key or serial number dependence. Applicant re-submits that Candelore et al. fails to

disclose generation of a machine identifier from the object identifier of the randomly deleted records as recited in Claim 1.

Concerning Claim 8 and the Examiners response on page 3 of the Office Action dated 4/3/6, columns 2, 19 and 24 of Candelore et al. are cited, as above, to indicate a teaching of generating a machine identifier based on locations derived from a list of records randomly deleted from a database of object identifiers as recited in Claim 8. The Examiner states that "underlying functionality achieved by the use of the database is disclosed in the Candelore patent i.e. storing the program in non contiguous memory". Applicant respectfully disagrees because storing a program in non-contiguous memory is not relevant to Claim 8 and "underlying functionality" is not the standard used for 35 U.S.C. §102 anticipation as stated in MPEP §2131. Applicant submits that Candelore et al. does not expressly or inherently teach generating a machine identifier based on locations derived from a list of records randomly deleted from a database of object identifiers as part of a method recorded on a machine-readable medium as recited in Claim 8. Applicants note that the aspect of random deletion of records from a database is not found in Candelore et al.

Concerning Claim 14, addressed on page 3 of the Office Action dated 4/3/6, columns 2, 19 and 24 of Candelore et al. are cited, as above, to indicate a teaching of a random number generator that selects dummy records to be deleted, and the locations of the deleted records added to the list of unused locations from which the machine identifier is generated as recited in Claim 14. Columns 2, 19 and 24 of Candelore et al. are cited as above for the "underlying functionality". Also noted are col. 15, lines 42-50 which read:

> "In another aspect of the present invention, a secure circuit uses program information for generating a cryptographic key. The key may be used to descramble a data transmission in hardware. Depending on the partitioning of the secure circuit, the descrambling may be done internally or externally.
>
> The key may be generated and handed to a software module to descramble the data transmission. The software module may be internal to the secure circuit or external to the secure circuit." (col. 15 lines 42-50).

Applicant notes that a "key" is not recited in Claim 14 and that Candelore et al. still fails to expressly or inherently teach a random number generator that selects dummy records to be deleted, and the locations of the deleted records added to the list of unused locations from which the machine identifier is generated as recited in Claim 14.

Simply, Applicant cannot find any teaching in Candelore et al. that can be regarded as a 35 U.S.C. §102 anticipation of independent Claims 1, 8, and 14. Specifically, Applicant can find no portion of Candelore et al. that teaches deletion of database records as part of generating a machine identifier. Without such a teaching, Candelore et al. cannot anticipate the pending claims because the elements are not present.

More specifically, Applicant submits that Candelore et al. does not disclose generating a machine identifier based in part on deleting database records in a database as recited in Claim 1. Applicant submits that Candelore et al. does not disclose generating a machine identifier based in part on locations derived from a list of records randomly deleted from a database of object identifiers as recited in Claim 8. And, Applicant submits that Candelore et al. does not disclose a random number generator that selects dummy records to be deleted, wherein the selected records are deleted, and the locations of the deleted records added to the list of unused locations from which the machine identifier is generated as recited in Claim 14.

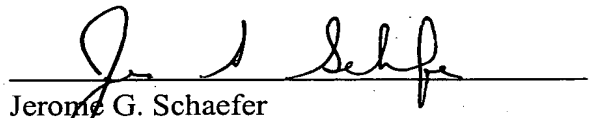
Since Candelore et al. does not teach all of the elements of independent Claims 1, 8, and 14, it cannot anticipate pending Claims 1, 5-10, and 12-17 under 35 USC §102(b). Applicants respectfully request withdrawal of the rejection of all pending claims as they patentably define over the cited art.

Conclusion

Applicant respectfully requests withdrawal of the 35 U.S.C §102 rejection and a Notice of Allowance for all pending claims as they patentably define over the cited art. Alternately, Applicant respectfully requests removal of the finality of the Office Action dated 4/3/6 because no claims are amended as part of this Office Action response and the cited reference cannot anticipate the pending claims.

Respectfully Submitted,

Date: June 1, 2006



Jerome G. Schaefer
Registration No. 50,800

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439